

- [0006] When a client is configured to use RADIUS, any user of the client presents authentication information to the client. This might be with a customizable login prompt, where the user enters a username and password. Alternatively, the user might use a link framing protocol such as PPP or EAP, which has authentication packets carrying this information. Once the client obtains such information, the client may choose to authenticate using RADIUS.
- [0007] PPP provides a standard method for transporting multi-protocol datagrams (packets of information, along with relevant delivery information such as the destination address that is sent through a packet-switching network) over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which can be used to negotiate authentication methods, as well as an Encryption Control Protocol (ECP), used to negotiate data encryption over PPP links, and a Compression Control Protocol (CCP), used to negotiate compression methods.
- [0008] EAP is a general protocol for PPP authentication that supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at a Link Control Phase. Rather, the specific authentication mechanism selection is postponed until an Authentication Phase. This postponement allows a PPP authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a "back-end" server, such as a RADIUS server, which actually implements the various mechanisms while the PPP authenticator merely acts as a conduit for the authentication exchange. Through the use of EAP, support for a number of authentication schemes may be added, including smart card, public key, one time password, etc. To date, however, EAP methods have focused on authenticating a client to a server. The EAP protocol allows a PPP peer to take advantage of the integrity-protected ciphersuite (scrambled or otherwise encoded text) negotiation, mutual authentication, and key management capabilities of the Transfer Level Security (TLS) protocol.

[0009] A smart card is a credit card-sized, tamper-resistant security device that offers functions for secure information storage and information processing that relies on Very-Large-Scale Integration (VLSI) chip technology. VLSI is generally considered to encompass the range from 5,000 to 50,000 components densely packed in an integrated circuit. A smart card contains a secure microprocessor chip embedded in the card. The chip can implement a secure file system, compute cryptographic functions, and actively detect invalid access attempts. With proper application of file system access rights, a smart card can be safely used by multiple, independent applications.

[0010] The basic principle of Public Key Infrastructure (PKI) technology is a mathematical concept that can be used to relate certain pairs of large numbers (called keys) in a special way. If one of the keys is used to encrypt a message, the other key can be used to decrypt the message, and vice versa. Fundamental to this scheme is that only these two keys (called a key pair) are related in this way. So, in other words, if a message is encrypted with one key, the message can be decrypted only by the matching key in the pair. One key is called a private key and the other is called a public key. The private key is known only by the user; the public key is published as widely as the user desires.

[0011] The following is an example of how a private message is sent from a sender to a recipient. The recipient's public key is used to encrypt the message, which is then sent to the recipient. The recipient uses his/her private key to decrypt the message. The sender knows that only the recipient can read the message because the message can only be decrypted using the recipient's private key. One concern with this arrangement is that the sender does not know whether the recipient's true public key is being used to encrypt the message. To overcome this concern, a certificate is employed.

[0012] A certificate binds a public key to an identity (and possibly other information about that identity). The sender and recipient share a trusted third party (e.g. a mutual friend, an organizational administrator, or a government agency). If the recipient goes to that trusted third party and proves his/her identity and presents his/her public key, that third party bundles and “signs,” or verifies the authenticity of the public key along with the recipient’s identity and any other appropriate information. This bundle of information is called a certificate, and the process of obtaining one is called certificate issuance.

[0013] A notable property of certificates is that public key tampering can be readily detected. The certificate is signed by the trusted third party (called a certificate authority, or CA). If the certificate is tampered with, the sender can tell because the CA is not recognized or the certification is improperly signed. Further, the sender can look at the certificate and verify that the certificate was, in fact, signed by the intended trusted third party. This mechanism assures that the recipient’s public key really belongs to the recipient, at least to the level that trust exists in the CA.

[0014] A security management system, for instance, Entrust/Entelligence developed by Entrust Technologies of Plano, TX, manages certificates, time stamping, encryption, digital signatures, and other security issues on behalf of users. Security management systems, such as Entrust/Entelligence, also have features such as automatic key and certificate management, and centrally managed policies and settings. Entrust/Entelligence integrates into a client computer environment. Also, instead of a separate log in procedure for each application stored on the computer, a user logs in only once to securely access all applications that are secured with a product such as Entrust/Entelligence.

[0015] Certificates used to verify a signed document may be stored on a server running a directory service. A directory service is a service running on a network